WatchGuard System Manager and Fireware™

Release Notes for WSM v10.2.12 and Fireware v10.2.12

Release Notes Revision Date: December 14, 2009
WSM build number: 248647
Fireware build number: 248545

Introduction

WatchGuard® is pleased to release WatchGuard System Manager (WSM) v10.2.12 management software and Fireware / Fireware Pro v10.2.12 appliance software.

The v10.2.12 release contains a number of defect fixes for issues reported by WatchGuard customers, as well as fixes for several vulnerabilities and improvements to Mobile VPN with SSL, Branch Office VPN and general stability. Also, in this release the Mobile VPN with SSL client has been updated to support Windows 7 and Windows 64-bit operating systems.

See the Resolved Issues section below for a complete list of resolved issues.

Before You Start

Before you install this release, make sure that you have:

- (IMPORTANT) Fireware or Fireware Pro v8.3 or later installed on your Firebox. If you have an earlier version of Fireware installed on your Firebox, you must upgrade to Fireware v8.3 or later before you install Fireware v10.2.12. See the Known Issues section for more instructions.
- (IMPORTANT) A backup copy of your current Fireware configuration file. To make a backup of the configuration file, see “Configuration Files” in the *WatchGuard System Manager User Guide*.
- (IMPORTANT) A full backup of the Fireware image or Firebox X WFS image. To make a backup of the image, see “Configuration Files” in the *WatchGuard System Manager User Guide*.
- An appropriate Firebox and the required hardware and software components as shown in “WSM v10.2.12 System Requirements” below.
- Feature key for your Firebox – If you are a new user, download this from the WatchGuard LiveSecurity site after you register your Firebox. If you have already registered a Firebox X Core or Peak e-Series and have not updated your feature key since v9.0 was released, download and save a new feature key for your Firebox to take advantage of changes in firewall throughput limits in the feature key.
- Documentation for this product is available at www.watchguard.com/help/documentation

WatchGuard System Manager v10.2.12 System Requirements

	If you have WatchGuard System Manager client software only installed	If you install WatchGuard System Manager and WatchGuard Server software
Operating System	Windows Vista (32-bit), XP SP2 (32-bit), Windows Server 2003 (32-bit)	Windows Vista (32-bit), Windows XP SP2 (32-bit), Windows Server 2003 (32-bit)
Browser	IE 6, IE 7, Firefox v3 and 3.5	IE 6, IE 7, Firefox v3 and 3.5
CPU	Intel Pentium IV	Intel Pentium IV
Processor Speed	1 GHz	2 GHz
Memory	1 GB	1 GB
Available Disk Space	250 MB	1GB

Downloading Software

To download WSM and Fireware v10.2.12:

1. Go to the LiveSecurity web site's Software Downloads page at http://www.watchguard.com/archive/softwarecenter.asp
2. Log in to the LiveSecurity web site. Then, select the product line you use and look for the WSM and Fireware v10.2.12 software download section.

Installation and Upgrade

Before you install the WatchGuard System Manager software, read the information in the Known Issues section below.

> ***Note*** The WSM v10.2.12 installer is not a full WSM install. To upgrade to WSM v10.2.12 you must have WSM v10.2 or later installed first. Review the WSM v10.2 release notes for the WSM v10.2 install instructions.

To upgrade to WSM and Fireware v10.2.12 if your Firebox is currently running WSM and Fireware v10.2.x

1. Back up your current Firebox image using **Policy Manager File > Backup**.
2. Close all applications and stop all servers using the WatchGuard toolbar before you start to uninstall WSM.
3. If you use a Management Server, make a backup of your Management Server configuration before you upgrade (right-click the Management Server icon and select **Backup/Restore**).
4. Launch WSM10_2_12.exe and follow the on-screen installation directions. Note: You must have WSM v10.2 or later installed before you run the WSM10_2_12.exe.
5. Launch the fireware10_2_12.exe and follow the on-screen installation directions.

6. To upgrade your Firebox to Fireware v10.2.12, use WSM v10.2.12 to connect to the Firebox. Use Policy Manager to open your Firebox X Peak or Firebox X Core configuration file.
7. From Policy Manager, select **File > Upgrade**. Browse to C:\Program Files\Common Files\WatchGuard\resources\Fireware\10.2.
8. Select the `FW1020B248545.wgu` file and click **OK**. Wait for the Firebox to reboot. You see a success message when the upgrade is complete.
9. After the image upgrade finishes, select **File > Save > To Firebox** to save the configuration to the Firebox.

To install the Fireware or Fireware Pro software for the first time on a Firebox X Core or Peak e-Series device

Use the instructions in the Quick Start Guide to install the software and do the initial configuration.

To upgrade a Firebox X Core from WFS to Fireware appliance software

Use the instructions in the Migration Guide to install this release. You can find a copy of this document at www.watchguard.com/help/documentation. If you currently use your Firebox as a Management Server, you must first upgrade to WSM/Fireware v8.3. After you migrate to WSM/Fireware v8.3 successfully, you can use the instructions above to complete the upgrade to WSM/Fireware v10.2, and then to v10.2.12.

- When you upgrade a Firebox X from WFS to Fireware, your current Gateway AntiVirus for E-mail and SpamScreen subscriptions stop. This is because these subscriptions only apply to a Firebox X running WFS.
- If you have a current GAV for E-Mail or SpamScreen subscription that has not yet expired, you can purchase the new Gateway AntiVirus/IPS and spamBlocker service subscriptions at a reduced cost. Contact your reseller for more information.
- All LiveSecurity and WebBlocker subscriptions continue with no change when you upgrade.

To install the v10.2 Mobile VPN with IPSec client software

There is no new v10.2.x Mobile VPN with IPSec client for this release. You can continue to use the v10.2 client, which you can download from the WatchGuard Software Downloads web site. The name of the file is `WatchGuard_EntryCl_Win_1010_059.exe`.

Or you can use the v11.1 Mobile VPN with IPSec client from the software download page. Follow the installation instructions in the release notes for the v11.1 Mobile VPN with IPSec client.

To install the v10.2.12 Mobile VPN with SSL client for Windows

The v10.2.12 Mobile VPN with SSL client is integrated into the Fireware 10.2.12 appliance software. Mobile VPN with SSL users can choose to download the v10.2.12 client from the Firebox or download the v10.2.12 client from the WatchGuard web site if the remote users do not have access to the Firebox on port 4100.

When a SSL client computer running an earlier version of the client software connects to a Firebox running v10.2.12, the user sees a prompt to upgrade the SSL client version to 1.17. Select **Yes** to upgrade the Mobile VPN client version to v10.2.12. Mobile VPN with SSL continues to operate if the user chooses not to upgrade, however, the user does not receive the fixes available in the v10.2.12 Mobile VPN with SSL client.

To install Single Sign-On (SSO) software

There is no change to the Single Sign-on agent software -- you can continue to use the v10.2.11 SSO agent software. There is no change to the Single Sign-On client software -- you can continue to use the v10.2.9 SSO client software.

To install v10.2.11 Single Sign-On agent software

1. If you are upgrading from an SSO implementation installed prior to v10.2.11, you must first uninstall the existing SSO agent.
2. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the Software Downloads page and download the WatchGuard Single Sign-On Agent 10.2.11. Save the WG-Authentication-Gateway.exe file to your hard disk.
3. Install the file on a domain computer with a static IP address running Microsoft Windows 2003, Windows XP, or Windows Vista and complete the setup wizard. It is a good idea to install the SSO agent software on your domain controller. For more setup instructions see the WSM/Fireware help system.

To install v10.2.9 Single Sign-On client software

1. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the Software Downloads page and download the WatchGuard Single Sign-On Client 10.2.9. Save the WatchGuard-Authentication-Client.msi file to your hard disk.
2. Because the SSO client installer is an MSI file, you can choose to automatically install it on your user's computers when they log on to your domain. You can use Active Directory Group Policy to automatically install software when users log on to your domain. For more information about software installation deployment for Active Directory group policy objects, go to http://www.microsoft.com. You can only install the client software on computers running Microsoft Windows 2003, Windows XP, or Windows Vista.

Resolved Issues

General

- This issue resolves an issue with our Active Directly authentication implementation. Previously, authentication to the Firebox on port 4100 could succeed without a password when a valid user name was used in the HTTPS authentication URL and the AD configuration on the Firebox used a valid "searching user" account. [41027]
- Fireware v10.2.x uses ISC's DHCP server to assign DHCP IP addresses. Some versions of ISC's DHCP server are affected by a Denial of Service (DoS) vulnerability and cannot handle specially crafted DHCP requests. Fireware v10.2.12 updates our implementation of the ISC DHCP server to correct this issue. For more information about this flaw, see http://xforce.iss.net/xforce/xfdb/51717. [40557}
- Fireware v10.2.x uses OpenSSL to implement the Secure Sockets Layer (SSL) protocol. Many SSL implementations, including OpenSSL, are affected by a SSL/TLS renegotiation vulnerability that attackers could leverage in man-in-the-middle (MitM) attacks. Fireware v10.2.12 updates our OpenSSL implementation. To correct this problem we disable TLS renegotiation. For more information about this flaw see: https://www.kb.cert.org/vuls/id/120541. [41351]
- An outside security researcher reported a minor Cross-Site Scripting (XSS) vulnerability in Fireware's web-based user authentication portal. Fireware v10.2.12 corrects this XSS vulnerability. [40784]
- This release resolves an issue that caused excess memory use on the Firebox when WSM polls the Firebox. [34568]

- This release resolves an issue that prevented the Firebox from maintaining a connection to the Log Server if data was sent before the SSL handshake with the server completed. [39662]
- A kernel crash with `eip:0010:[<e045f1bc>]` no longer occurs when you configure your Firebox in Drop-in mode. [40845]

Authentication

- The Active Directory search algorithm has been improved so that the Firebox now recognizes transitive group memberships. This is also commonly referred to as the user being in a "nested" group. For example:
  - A user is a member of GroupA
  - GroupA is a member of GroupB
  - The user is not directly a member of GroupB

  The new Active Directory search algorithm now sees the user as a member of GroupB because of the transitive relationship, even when the user is not directly a member of GroupB.

  Note that this functionality was previously available with Single Sign-On (SSO). The change applies to Mobile VPN with SSL, Mobile VPN with IPSec, and firewall authentication using the port 4100 portal. [29509]

Branch Office VPN

- This release resolves an issue that caused the IKED process to crash and all Branch Office VPN tunnels to fail. [39593] [41429]
- The IKED process no longer crashes when a Nessus Scan is performed through a Branch Office VPN tunnel. [40901]

Mobile VPN with SSL

- The Windows SSL VPN client has been updated to support Window7 and Windows 64-bit operating systems. [39841]
- The Mobile VPN with SSL client now successfully connects to a backup Firebox IP address if one is configured. [35256]
- If the `openvpn` process dies or is manually stopped the SSL client no longer uses up 100% of the CPU on the client computer. [39997] [41424]
- This release resolves an issue that caused the SSL client logon to fail if the user connected and disconnected the SSL client multiple times without closing the SSL client. [41425]
- This release resolves an issue that prevented the SSL client from releasing the assigned IP address. [39004]

Proxies

- When you use a caching proxy server, the Firebox no longer prevents an FTP session from a web browser from succeeding because of an HTTP proxy line parsing error. [41018]

Known Issues and Limitations

These are known issues for WatchGuard System Manager and Fireware v10.2.12. Where available, we include a way to work around the issue.

Upgrading to Fireware v10.2.12 from Fireware v8.2 and earlier

- It is not possible to upgrade directly to Fireware v10.2.12 from Fireware v8.0, v8.1, or v8.2.x. You must upgrade to Fireware v8.3 before you install Fireware v10.2.x.
- If you use Internet Explorer 6, the web-based Quick Setup Wizard can fail to complete the loading of software and initial configuration onto the Firebox because of the way IE6 handles old cache files and scripts.

> **Workaround**
>
> Clear the file cache in your web browser and try again. To clear the cache: from the Internet Explorer toolbar select **Tools > Internet Options > Delete Files**.

Quick Setup Wizard

- The Quick Setup Wizard installed on your management computer sets the IP address of the Log Server in the configuration file to the temporary dynamic IP address on the management computer during setup (10.0.1.100/24). [13908]

> **Workaround**
>
> Use the WSM-based Quick Setup Wizard only on a computer with a static IP address on which the Log Server is already installed.

Authentication

- The authentication applet does not load when you use an underscore character "_" in the URL path, such as https://xy_wz:4100. [27196]

> **Workaround**
>
> If you use a DNS entry for the Firebox, do not use the underscore character in the URL.

- When the check box to allow multiple logins is not selected, if there is a second login from a Mobile VPN with IPSec or Mobile VPN with PPTP after an initial login using a different authentication method, the first users is not correctly logged out. [37360]
- Windows 2000 Server no longer works for AD authentication.
- Users and groups must be in the search base, where previously only the user had to be within the search base.

SNMP

- Fireware v10.x does not support the HA-MIB used in Fireware v9.0 or older. [23998]

General WatchGuard Server Issues

- If you already have the WatchGuard Log Server or Report Server installed and you run the WSM installer again to install the Management Server for the first time, the task bar icon for the Management Server does not appear until you reboot. [27459]
- We recommend that you do not install server software on non-English Windows 2000.
- Both the Report Server and Log Server administrative user interface email configuration require you to enable the **Server Settings tab > Send a warning if the database reaches the warning threshold** setting, at least long enough to fill in the **Send warning message to** text box. All email notifications sent from the Log and Report Servers are sent to this address. The mail sender for all email sent by Log and Report Server is set in the Notification Setup section below the Expiration Settings tab. You must enable the **Turn on notification** check box and

complete the **Send email from** text box before any email notification messages can be sent from the server.

- The Management Server, Report Server, Log Server, and Quarantine Server share the same administrative password. If you restore a back up configuration to the Management Server, the administrative password changes for all servers. [22381]
- After you change the Master Encryption Key, all WatchGuard servers must be stopped and restarted. [27416]
- Servers that are stopped will restart after the computer on which the server software is installed reboots. [2752]

Workaround

Use the Windows Services applet (Start > Programs > Administrative Tools > Services) to set the Startup Type for the appropriate service to "Manual" if you do not want the service to start automatically on when the computer starts.

Quarantine Server

- Quarantine Server does not start if the logging directory is set to a non-existent directory. [23540]

Logging / Log Server

- **Maximum Database size** setting is for threshold notification only. This setting does not limit the disk space used by the Log Server database. [27338]
- The tool to convert log files from WFS 7.x format to XML is no longer included in WSM v10.x, because it is not needed in the v10.x logging/reporting systems. The new systems can create log files and reports for Fireboxes installed with WFS appliance software.
- If you install the Log Server on a computer running Windows 2000, you must install Windows Installer 3.1 and Service Pack 4 or the Log Server does not start. [24169]

Reporting/ Report Server

- When you create a group of more than 10 Firebox devices for combined reports, the Most Popular Domain report can have incorrect byte totals. [23838]
- When your Report Server is configured to send log messages to the Log Server, and both servers are on the same computer, the Boxes Under Management report appears in the list of Report Server reports instead of in the list of Management Server reports. [23834]
- When you cancel a “load report” operation in Report Manager it can take a very long time to stop. [22887]
- The Denied Packets Summary report shows a mismatch between the reported number of records processed and the total number of attempts denied in the summary. The last device to have packets denied is not shown on the report. [23805]
- The WSM Device Manager sends a log message with the time that it inserted a device in UTC format (YYYY-MM-DDTHH:MM:SSZ). This is incorrectly presented as the local time of the Report Server. The UTC information is stripped, but the timestamp is not converted to local time. [23822]
- If you do not have your email client configured before you try to email a report from Report Manager, the email is not sent and a Java exception pops up on your screen to indicate that Report Manager could not log in to the email client. [23774]
- We have made many improvements to reporting in the v10.x release. However, if you prefer to use the legacy Historical Reports tool available in previous releases of WSM, you must

continue to use your existing Log Server. The new Log Server is not compatible with previous implementations of Historical Reports. Customers, including those running appliances with WFS, who have grown accustomed to the existing report tool should thoroughly review the documentation before they upgrade to WSM v10.x.

WSM Centralized Management of Firebox X Edge devices

- The ability to configure Dead Peer Detection for Mobile User with IPSec is not available for centralized management. [29568]
- WSM cannot be used to configure the external interface of an Edge as a Wireless Client. [23081]
- The option to configure Mobile VPN with IPSec for a group is not available in WSM. [23097]
- WSM does not allow the configuration of only WAN1 or WAN2 in a multi-WAN enabled incoming policy for Edge. [23199]
- WSM does not support the configuration of 1-to-1 NAT on the Edge if the global configuration settings in WSM are enabled. [23251]
- When you configure the Mobile VPN with SSL Virtual IP address range, you must make sure that the IP address range does not overlap with those used for DHCP or PPTP. [22460]
- WSM does not change the Edge model type after you upgrade from an x10 to an x55 model in the device status tab. [15809]
- When Firebox X Edge devices are added to a centralized management configuration and changes are made that require a reboot, there is no notification that a reboot is required to apply changes. [11985]
- You cannot select WPA2 in the wireless configuration settings for Firebox X Edge e-Series devices running v8.6.x or v10.x. [21557]
- The 'Apply to VPN' option is not available under centralized management. There is a VPN-Any policy created for IPSec BOVPN traffic. [23195]
- Virus Outbreak Detection options appear on the Gateway AV/IPS page, but these options only apply to spamBlocker. [23180]

Management Server

- The Management Server **File > Import from File** feature does not work. To restore a Management Server configuration, use the **Backup/Restore** option available when you right-click the Management Server task bar icon. [27511]
- When a certificate for a managed Firebox is revoked, it does not show as revoked until the Management Server lease expires. [14041]
- The Management Server does not correctly recognize managed devices that use multi-WAN and have both static and dynamic external interfaces. A WSM v10.x Management Server only recognizes an Edge or Firebox X Core or Peak as static or dynamic -- but not both. Branch office VPN tunnels are created only to the first external interface when the Firebox has both static and dynamic external interfaces. [21416]
- A custom VPN policy template using AES encryption for phase 1 does not work with Firebox devices running Fireware v9.0 or earlier. Although the Management Server allows drag-and-drop tunnel creation between v10.x and pre v9.1 using AES for phase 1, the pre v9.1 Firebox will reject the configuration. [21627]
- If the Management Server is behind a Firebox configured in drop-in mode, and a branch office VPN is created to another Firebox configured in drop-in mode, the remote Firebox cannot contact the Management Server if the branch office VPN tunnel is not established. [21475]

- The default managed VPN tunnel configuration does not enable NAT-Traversal. [23756]
- When you use the default route VPN tunnel feature, all traffic from the remote networks will match the default 'ANY' policy created by the Management Server. This prevents remote branch office VPN traffic from matching other firewall policies configured at the central location. To force traffic to match specific policies at the central location, VPN templates must be used. The VPN template on the Management Server must include ports that match all traffic through the branch office VPN tunnel except traffic that should match firewall policies at the central location. [21965]

Firebox System Manager (FSM)

- When Firebox System Manager is connected to a Firebox for hours, there can be a small memory leak on the Firebox. [15518]
- The status of a managed branch office VPN tunnel between a Firebox X Core or Peak running Fireware v10.x and a Firebox X Edge running v10.x may not show correctly in Firebox System Manager. [23413]

WatchGuard System Manager (WSM)

- After you install WSM v10.2.x the **Start Menu > All Programs** display continues to show WatchGuard System Manager 10.2.
- When you upgrade from v9.x to v10.2.x, the **Setup > Logging > Advanced Diagnostics > Set all sub-categories to same level of detail** check box is cleared. [27514]
- WSM does not show the status of a PPPoE-based WAN interface if the Firebox is configured for multi-WAN. [19564]
- The NetMeeting packet filter does not work. Use the H.323 proxy policy to allow NetMeeting traffic to pass through the Firebox. [24281]
- When your Firebox is configured in drop-in mode, the Status Report incorrectly shows the external interface subnet mask as 255.255.255.0 regardless of the actual drop-in network subnet. [21458]

Networking

- If you have a static NAT rule that uses the alias of an interface, the static NAT rule does not work if you change the interface IP address. [23502]

  Workaround

  Remove the static NAT rule from the policy and replace it with one that uses the IP address of the interface alias.

- When a DHCP lease renewal occurs, some unusual log messages can appear. The lease renewal succeeds and the log messages can be ignored. The log message shows as: `Deny x.x.x.x x.x.x.x icmp-Dest_Unreach code(3) 1-Trusted Firebox icmp error with data src_ip=x.x.x.x dst_ip=x.x.x.x pr=dhcp/bootp-client/udp src_port=67 dst_port=68 src_intf='1-Trusted' dst_intf='0' cannot match any flow, drop this packet 176 128 (internal policy) rc="104"` [27364]
- When you use the DHCP server with secondary networks, the DHCP server IP address given to DHCP clients is the primary interface IP address and not the secondary interface IP address. [10365]
- There is a compatibility issue between Firebox X Peak models 5000, 6000, and 8000 using Intel's CSA bus-based MAC (i82547) and the Marvell PCI bus-based MAC (88E8001). Network interfaces may sometimes negotiate at 100MB instead of 1000MB. [13659]

- Forcing the interface link speed to 1000MB, Full or Half Duplex may result in a failed interface link speed negotiation. We recommend that you always use the option to auto-negotiate link speed. [21319]
- ICMP protocol unreachable messages do not pass through the Firebox. The option to allow Protocol Unreachable messages under **Setup > Global Settings > ICMP Error Handling** does not work. [21236]]

Proxies and Services

- When you use an FTP proxy policy, some active mode FTP commands can fail. FTP proxy log messages look like this when the problem occurs: `proxy[1854] 1:1193825662: ftp response '425 Can't open data connection.\x0d\x0a'` [22229]
- The default setting for the **Turn on logging for reports** option is not consistent in proxy policies. POP3 proxy traffic is logged by default, but all other proxy policies do not send log messages by default. This option controls whether proxy transaction details are shown in Traffic Monitor. [23259]
- QuickTime Video-On-Demand does not work through the HTTP proxy. [19112]
- Notification for application blocking on the TCP-UDP proxy does not work unless Intrusion Prevention is enabled for the same TCP-UDP proxy policy. [27305]
- When you enable the TCP-UDP proxy, outbound SIP connections are not correctly sent to the TCP-UDP proxy. [23546]

Workaround

Configure the SIP proxy to directly handle SIP connections.

- When you enable the TCP-UDP proxy, outbound FTP connections are not correctly sent to the TCP-UDP proxy. [23533]

Workaround

Configure the FTP proxy to directly handle FTP connections.

- The server session exit banner is made anonymous even when the **Hide Server Replies** check box is cleared in the POP3 proxy configuration. [23714]
- When you configure the SMTP proxy to strip Uuencoded and BinHex attachments, a small portion of the attachment header remains in the body of the email, together with the deny message. [22989]

Workaround

Disable stripping of Uuencoded and BinHex attachments.

- If you set the advanced logging level too high for the SMTP proxy and spamBlocker, the Firebox can become unstable when proxy traffic is at high levels. [21459]
- If a configuration contains multiple feature keys and one of the feature keys has expired, security subscriptions and signature updates fail after you upgrade to v10.x. [24050]

Workaround

Open your configuration in Policy Manager and go to **Setup > Feature Keys**. Click **Remove** one time to remove the expired feature key. Save the configuration to the Firebox.

- If you use multiple proxy policies on a Firebox X Core model X500, X700, X1000 and X2500, we recommend that you upgrade the Firebox memory to 512MB. Contact your WatchGuard reseller for information on how to purchase a 512MB memory upgrade kit.
- VoIP deployments are often complex and use many standard and proprietary protocols. Our current proxies only support standards-based traffic using the H.323 and SIP protocols, for basic voice, video, and data transfer. In VoIP industry terminology, these new proxies are more accurately called Application Layer Gateways (ALGs). Some proxy features, services, and configurations may not be supported with all types of VoIP hardware. These features include chat, whiteboarding, and fax transmission. Specific configuration limitations are noted below for each protocol. We strongly recommend that you perform compatibility and interoperability tests within your own organization before you deploy the H.323 or SIP proxy in a production environment.
- The H.323 proxy supports NAT traversal for voice and video traffic. However, support for H.323 Gatekeeper (PBX hosting/trunking) and T.120 multimedia is not included in this release. This limits use of the H.323 ALG to point-to-point scenarios, such as video conferences, that do not use an H.323 Gatekeeper server. While compatibility and interoperability cannot be guaranteed, point-to-point audio/video connectivity has been demonstrated with common software clients and video hardware.
- The SIP proxy supports NAT traversal for voice and video traffic. It does not provide the PBX registration capabilities of a typical standalone SIP Registrar-Proxy, but instead is transparent to SIP traffic. You must have your own Registrar-Proxy server to route PBX traffic, and this Registrar-Proxy server must be located on an external network. While compatibility and interoperability cannot be guaranteed, point-to-point audio/video connectivity and hosted audio connections have been demonstrated with common software clients.

spamBlocker

- If you use both spamBlocker with Virus Outbreak Detection (VOD) enabled and Gateway AV to scan your email and the SMTP proxy detects an email message that is both spam and a virus, the SMTP proxy applies the action that is configured for VOD to the message. Specifically, if the VOD action is set to **Strip**, then the attachment(s) are removed from the message and cannot be recovered. If the VOD action is set to **Lock**, the attachment is locked in the quarantined message. [23709, 23711; all platforms]
- When spamBlocker finds a Virus Outbreak Detection (VOD) indication for an email message, all of the email's attachments are stripped or quarantined. This includes the body of the email, if the sending client has sent it in HTML format. [23485, all platforms]
- When an infected email message with multi-part attachments (i.e., embedded email messages) is detected by VOD, and Firebox is configured with the **Strip** action, a small section of the email header in the attachment remains in the delivered attachment, together with the deny message for the attachment. This header information should cause no problems because viral content is always stripped. [23550, all platforms]
- The spamBlocker Proactive Patterns feature is not available for Firebox X Core models X500, X700, X1000, and X2500. Policy Manager allows the user to configure the proactive patterns feature for non e-Series Core Fireboxes, however, the feature does not work. [21496]

Gateway AV/IPS

- The Firebox System Manager Security Services tab only updates the **Available version** information for the AV engine, AV signatures, and IPS signatures once each hour. Because of this, the displayed available version can show as older than the installed version after a manual update. You must disconnect and reconnect FSM to the Firebox to refresh the Security Services information. [21639]
- When your Gateway AV configuration is configured to lock infected email messages, an email attachment is greater than 100K bytes, and a virus is detected after the first 100K bytes, then the attachment is truncated instead of locked, even though the log message shows that the file was locked. [21489]

WebBlocker

- You must download a new full WebBlocker database for your WebBlocker Server when you upgrade from WSM 9.x or older to WSM v10.x. The WebBlocker Server database has been upgraded from 40 to 54 categories. You must do this even if you chose to keep the WebBlocker database and configuration files from the previous version of WSM. Verify your WebBlocker profile configurations after the upgrade to make sure your profile to make sure they take advantage of the new categories.
- No deny message is sent back to the client when an HTTPS connection is correctly blocked because of your WebBlocker configuration. Blocked HTTPS connections are accurately recorded in the log file. [22515, all platforms]
- If you have a v9.1 WebBlocker configuration with the **Deny All Categories** check box selected, the check box is cleared when you upgrade to WSM/Fireware v10.x. [23679]

> **Workaround**
>
> After you upgrade from v9.x or older to WSM/Fireware v10.x, you must select the **Deny All Categories** check box again and save the change to the Firebox.

User Interface

- The WSM v10.2.x software includes many bug fixes that do not affect the user interface. Any changes to the user interface included in the v10.2.x release are not localized. If you upgrade from the localized v10.1 release to the v10.2.x release, note that new UI elements remain in English. There are no updates to the localized help content.

Branch Office VPN

- If multiple IKE Phase 1 and Phase 2 proposals are configured in Policy Manager, Fireware only sends the first IKE proposal when it initiates a VPN tunnel. If Fireware does not initiate the VPN tunnel, Fireware cycles through the list of proposals until a match is found. Because of this issue it is important to have the order of the phase 1 and phase 2 proposals match on both sides of the VPN tunnel, if multiple proposals are used. [24834]
- When a certificate is revoked or renewed, a managed branch office VPN tunnel with a valid certificate does not appear when you start a Fireware device in drop-in mode. [11409]

> **Workaround**
>
> Use WSM to remove the managed Branch Office VPN tunnel and then create the tunnel again.

- Beginning with the v8.3 release, you cannot use non-ASCII characters in branch office VPN shared keys. The UI does not allow you to enter non-ASCII characters in the shared key field.

Mobile VPN with IPSec

- At the end of the Add Mobile VPN with IPSec Setup Wizard, the check box to add users to the group may not be visible. [27554]

Workaround

To see the check box, expand the window size of the Setup Wizard.

- On very rare occasions, a large FTP transfer from a remote Mobile VPN client can get dropped. Specifically, this can occur if a transfer is disconnected during the phase 2 rekey. The client reconnects using the 2nd phase 2 Security Association (SA), and packets arrive from the second SA before packets from the first SA are dropped. [12340]

Workaround

Set the Phase 2 Proposal Forced Key Expiration threshold for byte count to 0 and increase the timeout setting.

Mobile VPN with PPTP

- When you configure Mobile User with PPTP, the lower half of the configuration page may not be available. [27621]

Workaround

Expand the window size to restore the full configuration page.

- When the PPTP client connects to the Firebox, the connection-specific DNS suffix is not assigned [17394]

Mobile VPN with SSL

- The Mobile VPN with SSL client v11.x is not compatible with an e-series Core or Peak running v10.2.x.
- After the Mobile VPN with SSL client first connects, any subsequent changes made to the Mobile VPN with SSL configuration will cause a connection problem with Windows Vista SP1 clients. The client appears to connect correctly, however the client sends a log message that it unsuccessfully flushed the ARP table. [29621]

Workaround

There are 2 options to work around this issue:

1. Disable User Account Control (UAC) on the Vista PC; or

2. Go to Program Files >WatchGuard >WatchGuard Mobile VPN with SSL and right-click `wgsslvpnc`. Select **Run as Administrator**.

- The Mobile VPN with SSL client can fail to connect when it is configured to have routes to 12 or more networks. The client has a limit to the number of routes it can support related to the client configuration size. The route limit is not exact, but, depending on data in the configuration the limit is approximately 12 to 25 routes. [24226]
- The Mobile VPN with SSL client can fail to stay connected if the client computer has more than one active network interface. [27112]
- You cannot use extended ASCII characters (ä,ö,ü,ß) in a user name for Mobile VPN with SSL Active Directory authentication. [23647]

- You cannot install the Mobile VPN with SSL client on a Windows 2000 Pro computer. [22550] [23667]
- The SSLVPN Any service cannot be removed when Mobile VPN with SSL is enabled, [24656]

Workaround

To add custom policies for Mobile VPN with SSL users, you can disable the SSLVPN Any policy and add custom policies.

User Documentation

Documentation changes for the WSM/Fireware v10.2.12 release are included in the most current English help system available at www.watchguard.com/help/documentation. There is no updated WSM User Guide for this release.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or on the Web at http://www.watchguard.com/support. When you contact Technical Support, you must supply your registered Product Serial Number, LiveSecurity key or Partner ID.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375

Issues Resolved in Earlier 10.2.x Releases

For your convenience, this section shows a list of resolved issues from the release notes of all versions of 10.2.x prior to this one. For installation information, tech notes, and known issues for each of these releases, download the complete release notes for that specific release.

WSM/Fireware v10.2.1 Resolved Issues

Authentication

- For our customers who use Mobile VPN with IPSec with Vasco 2-factor authentication, the Firebox now correctly associates users with groups. Now, the Firebox matches the group name returned by the RADIUS server, as long as the correct group name is present in the Authentication > Group configuration in Policy Manager. After a user is authenticated, policies based on group association now work correctly for that user. [26819]

Note The value for the Filter-ID attribute must match the name of the Mobile VPN with IPSec user group or Mobile VPN with IPSec authentication fails. If you use two-factor authentication for firewall authentication (port 4100 connection to the Firebox using a browser) to filter access to Fireware policies, then the value of the Filter-ID attribute must match the name of a group you use in your policies to enforce authentication.

- Resolved an issue that allowed successful authentication from the Mobile VPN for SSL client for a user who is not in the SSLVPN user group but is part of another group on the Firebox. The user must now belong to the SSLVPN user group to authenticate to the Firebox with the Mobile VPN for SSL client. [25790]

WatchGuard System Manager (WSM)

- Dead Peer Detection is no longer enabled by default for pre-existing BOVPN tunnels after upgrading from 9.x to 10.2.1. [27899]

Firebox System Manager (FSM)

- HostWatch no longer displays zero connections when a HostWatch view filter check box is cleared. [27568]

Mobile VPN with SSL

- When you use Mobile VPN with SSL and Firebox authentication, you can now use a # character as the first character in a password. [25499]

Proxies

- The HTTPS proxy no longer crashes when the SSL endpoint responds to an SSL connection with no domain. [27983]
- The SMTP proxy and POP3 proxy no longer strip attachments with extra padding characters from base64-encoded messages. [27445]

Upgrade issues

- The Firebox no longer crashes during an upgrade from Firebox v10.1 when you use 1-to-1 NAT with VLAN. [27758]

Reporting/ Report Server

- When you clear the Windows Event Log option on the Report Server Administration Logging tab, logging to the Event Log is now correctly disabled. [27795]
- The predefined report category no longer shows up multiple times in a report. This fix applies only to new installations of the v10.2.1 Report Server. For customers currently experiencing this issue, you can either contact WatchGuard Support for a script that will fix the problem in the Report Server database or you can uninstall and reinstall the Report Server, making sure to remove all data associated with the Report Server installation. [27815]
- The Report Server no longer fails to generate the HTTP URL Detail report with the following log message: `Error (8203), Exception get_http_url_detail_records().`[27811]

Logging/ Log Server

- The logging process now restarts the connection between the Firebox and the Log Server if the SSL connection between the two devices is in a waiting state for more than 90 seconds. This resolves an issue that caused the Firebox to stop sending log messages to the Log Server because it did not correctly detect that the connection was stuck in a waiting state. [27788]
- After you upgrade to v10.2.1 from a previous v10.x version, Report Manager no longer fails to start because the directory location for report definition files points to the previous version. [27624]
- A bug that caused the Log Server to crash with a high number of concurrent logging connections has been resolved. [27343]
- An issue that caused the Log Server to fail to start after you upgrade from v10.x to v10.2.x has been resolved. [27775]

WSM/Fireware v10.2.2 Resolved Issues

Authentication

- Resolved memory leak in the authentication feature code. [28417]

WatchGuard System Manager (WSM)

- The sticky connection settings for Server Load Balancing no longer reset to the default (8 hours) after you save the configuration. [27833]
- The default values for Mobile VPN with PPTP's MTU and MRU settings are now set to 1400. This improves interoperability with some applications through a PPTP-based VPN tunnel. [27316]

Reporting/ Report Server

- The denied packet summary report and the SMTP Proxy summary report now show only the top 50 records to allow for better presentation of the data. [28328]

Logging/ Log Server

- Resolved an issue with the LogViewer Search Manager that caused search queries based on the Additional Info Column to return no information. [28067]

VPN

- The default branch office VPN settings are now the same for both Fireware v10.2.2 and Edge v10.2.2. This was done to make it easier to set up new BOVPN tunnels. [27979] [28389]

Networking

- Traffic on Ethernet ports 4 - 7 on Firebox X Core and Peak e-Series devices no longer fails with log message `invalid IP packet detected by device, firewall drop`. This issue resulted in High Availability instability when ports 4 - 7 were used for the HA heartbeat. [23817] [25947]

WSM/Fireware v10.2.3 Resolved Issues

WatchGuard System Manager (WSM)

- Windows Vista Enterprise no longer prevents Policy Manager from starting when a Firebox administrator logs into the management station with a different account from the account used to install WSM. [27450]
- When you use the Edge centralized management feature, the configuration page for LDAP and RADIUS authentication is no longer disabled when the **Require User Authentication** check box is cleared. [29339]

Reporting/ Report Server

- You can now apply filters to the reports created by the v10.x Report Server. There are no new reports produced, but you can now filter the data that appears in reports. [28729]

Logging/ Log Server

- Resolved an issue with the LogViewer Search Manager that caused search queries based on the "Additional Info" column to return no information. [28067]

Note This issue was mistakenly reported as fixed in the v10.2.2 release.

Quarantine Server

- Email sent to the Quarantine Server in HTML or Rich Text format no longer shows up as plain text when released from the Quarantine Server. [28058]

SMTP Proxy

- The SMTP proxy now sends a 200 success message when spamBlocker is configured to quarantine email that matches a spamBlocker exception. A 200 success message is also sent when spamBlocker is configured to quarantine email classified as spam, bulk, suspect or VOD. Sending a 200 success message back to the sending email client helps to prevent duplicate emails on the Quarantine Server. [29332] [29333]

Mobile VPN with IPSec

- The Session and Idle timeouts configured in Policy Manager for Mobile VPN with IPSec are now enforced if the authentication server sends no attributes for session and idle timeout. [19657]
- Iked no longer crashes when there are multiple Mobile VPN with IPSec clients authenticated to the Firebox from behind the same remote device performing NAT. [27748] [28601]

Mobile VPN with SSL

- The Mobile VPN with SSL client now supports Window Vista SP1. [27901]
- The Mobile VPN with SSL client and gateway now protect against "Man in the Middle" attacks. The Mobile VPN with SSL gateway generates a self-signed x.509 certificate when an IP address is assigned to the external interface of the Firebox. This certificate is presented by the gateway the first time a v10.2.3 client connects.
  Because the certificate is self-signed, a warning message about an “un-trusted” certificate is presented to the user the first time they connect to the Firebox. The user is given the option to confirm the certificate as trusted and save the certificate locally. Accepting the certificate as “trusted” allows the SSL client to warn the user if the certificate changes to alert the user of a possible Man in the Middle attack. [27304]

Single Sign-On

- Non-ASCII characters in the domain name no longer cause authentication to fail with log message `Malformed "list" response from SSO Agent`. The v10.2.3 SSO agent is required to resolve this issue. [27198]

Networking

- Fireware now supports the PPPoE configuration in which the ISP provides a block of public addresses to use behind the Firebox (a /29 network, for example) but assigns the network address for the subnet to the external interface of the Firebox. [27823]

WSM/Fireware v10.2.4 Resolved Issues

General

- SNMP system uptime no longer stops at 248 days. The system uptime now continues to increment to 497 days and then re-starts the count from zero. [29753]
- The language selection option during the WSM installation procedure now displays the Japanese language selection in Japanese instead of English. [30265]

WatchGuard System Manager (WSM)

- The wgauth_admin tool has been removed from the Management Server. This tool allowed a user that was logged in to the Management Server to get and change server management passphrases and log encryption keys. [30429]

Reporting/ Report Server

- You can now run WebBlocker reports for Fireboxes running WFS. [28596]

Logging/ Log Server

- To reduce the amount of log messages sent to the Log Server, the Firebox no longer sends log messages for denied ESMTP by default in SMTP and POP3 proxy policies. [29700]
- You can now change the log encryption key without using the previous log encryption key. [28730]
- The Firebox now sends a log message when its time is synchronized to an NTP server. [13038]

HTTPS Proxy

- The idle timeout in the HTTPS proxy is no longer treated as a session timeout. [28706]

Authentication

- Authentication on port 4100 no longer supports SSLv2 and now meets Payment Card Industry (PCI) compliance standards. [29863]

Single Sign-On

- The Single Sign-On solution is improved with the v10.2.4 release. A Single Sign-On client is now available to install on each computer in a network to improve the accuracy of who is authenticated. See the client installation instructions above for more information.
- The authenticated users list is no longer reset every 2 minutes. Each reset required the list of users to be queried again. On networks with more than 100 authenticated users, access through the Firebox was interrupted during the re-query. [27965]

WSM/Fireware v10.2.6 Resolved Issues

General

- SNMP system uptime no longer stays at zero. [31399]
- SNMP no longer crashes when SNMP traps are enabled. [31110]
- Bandwidth meter no longer stops displaying data. [31392]
- Mobile VPN with IPSec connections no longer disconnect when you save a configuration to a High Availability pair. [27928]
- PPPoE successfully negotiates after you reboot the Firebox when a secondary external IP address is configured. [30812]

WatchGuard System Manager (WSM)

- Schedules applied to policies now terminate active sessions when the schedule expires. [29223]
- The Management Server Setup Wizard and administrative UI have been changed so that the forward slash (/) character is no longer supported in either the organization name or the common name for the CA certificate. In earlier versions, the UI accepted the forward slash, but the Management Server then failed to start. [27898]

Reporting/ Report Server

- The URL detail report by client now shows the client user name instead of the IP address. [29535]
- The date shown on the report title now corresponds to the date range of the data in the report. Previously the report title showed the date the report was generated. [28295]
- Fixed a memory leak in Report Server that caused report creation to fail with an exception stack trace and also caused reports to run very slowly. [29087] [28565]

HTTP Proxy

- The HTTP proxy no longer performs a body scan for both IPS and Gateway AV when both security features are enabled. When both Gateway AV and IPS are enabled, body content scanning occurs only for Gateway AV. IPS uses the results of the Gateway AV body content scan. This improves throughput because the redundant scan is eliminated. [28002]

Single Sign-On

- SSO exceptions now work correctly. [27964]

Mobile VPN with SSL

- We now support the following character set on the Firebox authentication page for Mobile VPN with SSL: 0-9, a-z, A-Z, and the characters. _ - @. If you type a character outside this set, you get a message that the character is not valid. This helps to prevent injection attacks. [30538]
- If the Mobile VPN with SSL client cannot access the Firebox on port 4100, the client no longer waits a long time to connect. [30570]
- When you start the Mobile VPN with SSL client, the DNS client service on that computer now stops and restarts to update the computer to use the DNS server IP address provided in the Mobile VPN with SSL client configuration. [28120]

WSM/Fireware v10.2.7 Resolved Issues

General

- This release resolves a kernel crash associated with branch office VPN and Mobile VPN with IPSec traffic through the Firebox X Core or Peak e-Series. [29491]
- The Firebox no longer stops passing traffic when you save a configuration. [27821]
- Policy Manager no longer prevents the entry of host ranges for 1-to-1 NAT on the BOVPN tunnel route settings page. [30010]
- The Server Load Balancing feature in Fireware now correctly detects that a server is not responding and stops sending traffic to that server. [27276]

WatchGuard System Manager (WSM)

- You can now apply QoS and a schedule when you create a VPN firewall; policy template for managed BOVPN tunnels. [10270]
- You should no longer see the error message "*HTTP response code: 500 for URL https://x.x.x.x:4117/cmm/cmd*" when you try to connect to WSM. [29336]

High Availability

- If there is an active Mobile VPN with PPTP tunnel connected to the Firebox during a configuration save, Firebox System Manager no longer shows the HA peer status as "in-transition." [27557]

- WSM and Firebox System Manager connections no longer fail after a configuration save to two Fireboxes configured in an HA configuration. [31990]

Mobile VPN with SSL

- The Windows SSL VPN client no longer fails to install on Windows XP with a Runtime Error message. [31932]
- The Windows SSL VPN client now operates correctly after a computer returns from sleep mode. [31523]

WSM/Fireware v10.2.8 Resolved Issues

General

- This release resolves several stability issues on Firebox devices that have the upper 4 ports in use. [27896] [29899] [30057] [30093]
- You can now connect to a Firebox with WSM or Firebox System Manager more reliably after running a high load on the Firebox for several days. [35309]
- The time it takes to save a configuration is reduced as much as 60% when there are many policies. [27791]
- The Firebox can continue to operate even when IPS is using 100% of the CPU. [31361]
- Support files are now correctly rotated so they do not take up so much storage space. [33551]

Networking and VPN

- This release fixes an instability issue with PPPoE. [29212]
- The Firebox no longer stops getting OSPF routing table information from neighboring networks. [27202]
- The IKED process no longer becomes non-responsive when two users log in with the same name and same IP address. [33067] [33361]
- The MIA process no longer crashes during a configuration save when multiple mobile VPN users are logged in. [33617]
- Users now can use Mobile VPN (SSL, PPTP, and IPSec) with a dynamically addressed external interface without using DynDNS. [32707] [32715] [32716]
- You can now use a space in user names configured on the Firebox. [33687]
- Server Load Balancing now detects the revival of a dead server within 30 seconds instead of 10 minutes.

WatchGuard System Manager (WSM)

- The traffic load gauge on Traffic Monitor no longer incorrectly shows 100% even when the load is low on Firebox X Peak e-Series devices. [27950]
- The Firebox System Manager Traffic Monitor function “highlight search results” is now case insensitive. [33318]
- The sender address is now shown in Log Server alarm/notification emails. [31489]
- The Report Server can now generate POP3 reports. [332974]
- Devices are now correctly marked as connected when you use multiple Log Servers. [31524]
- The spamBlocker report no longer incorrectly reports 100% bulk mail. [28562]

Single Sign-On

- The SSO login information on the Authentication List now refreshes immediately.[31856]
- The SSO agent no longer crashes with Windows Event message: `EventType clr20r3`. [32775]
- The SSO client now returns the correct domain name.
- The SSO client and agent now handle both AD domain name information and NetBIOS domain name information correctly.
- The SSO client and agent now respond correctly to unexpected disconnections that occur within 10 seconds.

High Availability

- HA monitoring on external fiber interface now works correctly. [32967]
- When you enable HA, it no longer causes a branch office VPN rekey to occur approximately every two minutes. [33402]
- HA failover now occurs immediately when a critical process fails. [33823]

Mobile VPN with SSL

- The SSLVPN daemon no longer fails when you enter an empty password or a very long password. [31894] [35183]
- The Mobile VPN with SSL Mac OS X client now shows the Bound IP Address and Gateway Connected IP Address correctly. [34561]
- The Mobile VPN with SSL Mac OS X client now removes the search domain and DNS information when it is disconnected or you exit. [34564]
- The Mobile VPN with SSL Mac OS X client now shows both WINS addresses. [34560] [23635]
- The Mobile VPN with SSL Mac OS X client now sets the default log level to low. [34563]
- Routes of available networks are now correctly added when you install the Mobile VPN with SSL client software on a computer running Windows Vista. [34558]

WSM/Fireware v10.2.9 Resolved Issues

Server Load Balancing (SLB) and VPN

- A Firebox configured for server load balancing no longer stops sending traffic to a healthy server because of quick continuous requests, a missing route to a dead server, or interference from other SLB policies [35761]
- A Firebox configured for server load balancing now considers a server as active as soon as it can set up a connection with the server, instead of waiting for three successful tries. [35550]
- A problem that caused an IKED runtime crash with a pstack call trace"EIP:<e045684d>" is fixed. [32966. 36424]
- The Mobile VPN with SSL client can now resolve host names on an internal DNS server. [28120]
- If you have configured two DNS or WINS servers, both IP addresses are now assigned correctly to Mobile VPN clients (IPSec and PPTP). [12575, 33904]
- A problem that caused an error " HTTP response code: 500 for URL: https://x.x.x.x:4117/cmm/cmd" when you saved a configuration in which Mobile VPN with SSL is enabled has been fixed. [28105]

High Availability

- The primary HA Firebox no longer stays in the "in-transition" state indefinitely after you do an HA sync operation just after you save your configuration. [36033]
- HA sync now completes successfully when two HA ports are used. [30207]
- You can now use WSM to quickly create successive tunnels on Fireboxes in an HA pair and not lose management access. [36007]
- VRRP logging messages no longer show in the log file unless the appropriate log level has been set. [35763]

Single Sign On

- You can now install the SSO client on Windows Vista. [35869]
- When you enable SSO, you can now obtain group information even if the SSO agent is not installed on the Domain Controller. [36043]
- When you install the SSO client on Vista, you can now see the build number. [36289]
- SSO client and agent communication is now more reliable and several timeout issues have been resolved. [35199, 35200]
- SSO now ignores group names exceeding 32 characters and continues to process other group names. It no longer returns a "domain name str too log" error. [35988]

WSM Management

- WSM no longer displays a device as "Pending" when it is not. [36080],
- WSM can now handle different devices with identical IP addresses. It no longer shows a "Maintenance Alert" warning for these devices. [36068]
- LogViewer can now display SMTP and POP3 log messages whose headers are encoded in ISO-2022-JP. [33460]
- Firebox System Manager and Policy Manager now show and error that says "Invalid login/password" instead of "No SID" when users enter the wrong password when downloading a configuration, downloading a feature key, or during a system backup. [36959]
- Service Watch can now reliably connect to the Firebox when there are a large number of policies. [37142],

Proxy

- The Application Blocking feature now blocks the most recent versions of Yahoo!® Messenger. [36268]
- The Firebox now supports more than 1000 FTP proxy connections. [35998]

WSM/Fireware v10.2.10 Resolved Issues

General

- The Firebox now passes traffic that includes unkeyed GRE packets. [39088]

NAT

- Fireware now includes support for NAT loopback. NAT loopback allows a user on the trusted or optional networks to get access to a public server that is on the same physical Firebox interface and same subnet by its public IP address or domain name. [15513]
- You can now enable global and per-policy NAT for branch office VPN traffic. [38019]

- You can now specify IP addresses in the dynamic NAT configuration for branch office VPN tunnels. [38022]
- Static NAT and 1-to-1 NAT now operate with tunneled networks (tunnel switching with a zero or 0.0.0.0 route). [26764]

Server Load Balancing

- Server Load Balancing now operates correctly with global and per-policy dynamic NAT. [38018]
- The Server Load Balancing custom sticky timer now operates correctly. [39061]
- The Server Load Balancing least connection option now operates correctly. [38456]
- Server Load Balancing has been enhanced to improve the availability of service when servers start or stop.

Management

- You can now use the Wlimport.exe tool to import log files that contain ISO-2022-JP characters to your log database. [37771]

VPN, PPTP, and GRE

- Branch office VPN and Mobile VPN with IPSec now operate correctly when your Firebox is configured with a drop-in configuration. [38459, 38872]
- A problem has been fixed that prevented PPTP from working when the PPTP connection passed through a device that applied NAT. [17143]
- Mobile VPN with SSL traffic no longer stops when there are many SSLVPN sessions. [38928]

Proxy

- The SMTP proxy no longer hangs when it cannot contact the Quarantine Server. [27750, 34396]
- FTP downloads no longer stop before the download is complete when you use the FTP proxy with Gateway AV. [36074]

Vulnerability and Stability Enhancements

- When you use an LDAP server for certificate validation and the server is reachable for LDAP queries, WSM no longer loses Firebox connections. [33634]
- After a Firebox runs for 497 days without a reboot, network connections and the console port now continue to operate correctly. [35870]
- The lighttpd component used in Fireware has been upgraded to v1.4.22 to resolve several vulnerabilities in the previous lighttpd open source component. [38807]
- Several problems resulting in kernel crashes (EIP=fcd1c4a8 and EIP=e0057a43) are fixed. [38141, 36188]
- A problem that caused a kernel dump [c01356b3] when using the upper four ports on a Firebox has been fixed. [38862]
- A problem that caused the CMM component to crash and then automatically restart has been fixed. [37563]

WSM/Fireware v10.2.11 Resolved Issues

General

- The stability of network interfaces 4 through 7 on Firebox X Core and Peak e-Series devices has been improved. This improvement was also included in the Fireware v10.2.10 release. The primary symptoms resolved by the improvements are kernel stack traces and traffic not passing through interfaces numbered 4-7 for short periods of time. [36946] [39134] [36684] [30943] [30057] [33605]
- This release resolves a kernel crash related to using multi-WAN with a high number of concurrent connections. [36494]
- This release resolves a kernel crash when upgrading from v10.2.9 to v10.2.10 with both High-Availability and Drop-In mode enabled. [39676] [39616]
- This release resolves a kernel crash related to branch office VPN traffic. [40002] [40443]
- The ISC DHCP client used in Fireware has been improved to address a 'Stack Buffer Overflow' vulnerability reported as US-CERT VU#410676. [39073]
- This release resolves an issue that caused the Firebox LCD screen to stop updating. [39377]

Authentication

- The Single Sign-on group string length has been increased to support more than 64 groups. To support the larger number of groups, you must use Fireware v10.2.11 and the SSO agent v10.2.11 software. [39596]

Networking

- This release resolves an issue that prevented the Firebox DHCP server from renewing IP addresses after a DHCP lease expired. [39663]
- Traceroute now passes through the Firebox correctly. [39600]
- This release resolves an issue that prevented the CheckPoint VPN client from working correctly from behind a Firebox configured with PPPoE on its external interface and IPSec passthrough enabled. [39498]

Management

- This release resolves an issue that caused Policy Manager to not open the configuration from a Firebox. This problem resulted in an error that looked like this: `Server returned HTTP response code: 500 for URL: https://x.x.x.x:4117/cmm/sync/cli.` [38844]
- Policy Manager no longer requires that the External to Trusted1-to-1 NAT entry is added before the Trusted to External 1-to-1 NAT entry when you configure NAT loopback. [39275]

Branch Office VPN

- 1-to-1 NAT through a branch office VPN tunnel no longer fails when you use an IP address from the external interface but not add it as a secondary IP address on the external interface. [39666]
- This release resolves an issue that caused the IKED process to crash and caused all IPSec VPN tunnels to fail. [39476] [39585]

Mobile VPN

- The v10.2.11 Mobile VPN with SSL client resolves an issue that caused the client to fail to connect when you use Windows Vista. [34578]

- Mobile VPN with IPSec now works correctly when you use a Firebox configured with a drop-in configuration. [39777] [39708]
- Dynamic NAT is now applied correctly to Mobile VPN with IPSec traffic configured to route in through the Firebox and then back out to the Internet. [35955]

Log Server

- This release resolves a memory leak in the Log Server. [39479]